AUDIT KEAMANAN SISTEM INFORMASI BERDASARKAN STANDAR ISO 27001 PADA PT. BPR JATIM

[1)]Fine Ermana [2)]Haryanto Tanuwijaya [3)]Ignatius Adrian Mastan

S1 / Jurusan Sistem Informasi, Sekolah Tinggi Manajemen Komputer & Teknik Komputer Surabaya
email: 1)finermana@yahoo.com 2)haryanto@stikom.edu 3)Ignatius@stikom.edu

Abstract: Information security management is extremely important for the head office of PT. BPR JATIM, since all report originating from branch offices throughout East Java will be sent to the center every day and network security in data transmission allows the risk of loss of confidential company data. Core Banking System operates online using the server at the vendor. However the central office still get regular reports from the branches that still have to have a data server backup and recovery. Given the importance of information, the information security police should include procedures for asset management, human resources management, physical and environmental security, logical security, operational security and information technology in information security incident handling.

To find out how security information is in progress at the company, the need for security audit information system at PT. BPR JATIM to ensure that information security is implemented in accordance with the procedure. The standards used are ISO 27001 is selected because is very flexible depending on the needs of the organization developed and focused on information security management system.

The result of the audit of the maturity level of the overall value of 2,90 which means that security controls are located on level 2 planned and tracked, but has approached the level 3 well defined which is the level expected by company, necessitating increased security controls that have been recommended.

Keywords: audit, information security, ISO 27001, maturity level.

Manajemen keamanan informasi sangatlah penting bagi kantor pusat PT. BPR JATIM, karena seluruh laporan yang berasal dari kantor cabang di seluruh Jawa Timur akan dikirimkan ke pusat setiap hari dan keamanan jaringan dalam transmisi data memungkinkan resiko kehilangan data rahasia perusahaan. Transmisi data dan informasi tersebut menggunakan jasa salah satu *Internet Service Provider* (ISP) lewat jaringan *Virtual Private Network* (VPN). Sistem perbankan atau *Core Banking System* (CBS) pada PT. BPR JATIM menggunakan produk salah satu vendor Teknologi Informasi (TI) yaitu Sarana Transaksi Keuangan (SATU) yang beroperasi secara online namun masih menggunakan server yang ada pada vendor. Meskipun demikian, kantor pusat tetap mendapatkan laporan rutin bulanan yang berasal dari cabang sehingga tetap harus memiliki server data untuk *backup* dan *recovery* yang berjalan dengan baik.

Mengingat pentingnya informasi, maka kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya terdapat prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan *logical security*, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi (Direktorat Penelitian dan

Pengaturan Perbankan, 2007: 52). Untuk itu diperlukan audit keamanan sistem informasi pada PT. BPR JATIM untuk memastikan keamanan informasi diterapkan sesuai dengan prosedur. Standar yang digunakan yaitu ISO 27001. Beberapa hal penting yang patut dijadikan pertimbangan mengapa standar ISO 27001 dipilih karena dengan standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi serta ISO 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi SMKI yang diakui secara internasional yang disebut Information Security Management System (ISMS) certification (Sarno dan Iffano, 2009: 59).

LANDASAN TEORI

Audit

Audit didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (ICASA dalam Sarno, 2009: 3).

Audit Sistem Informasi

Weber dalam Sarno (2009: 28) mendefinisikan Audit Sistem Informasi sebagai proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif.

Keamanan Informasi

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimasi resiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis (ISO 27001 dalam Sarno dan Iffano, 2009: 27).

Sistem Informasi

Sistem Informasi (SI) adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi

dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan (Leitch dan Davis dalam Jogiyanto 2005: 11).

ISO 27001

ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan. Sarno dan Iffano (2009: 187) mengatakan kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (*security control clauses*), 39 objektif kontrol (*control objectives*) dan 133 kontrol keamanan/ kontrol (*controls*).

Maturity Level

Penilaian *maturity level* mengunakan SSE-CMM. Menurut Gunawan dan Suhono (2006: 136), SSE-CMM adalah *Capability Maturity Model* (CMM) untuk *System Security Engineering* (SSE). CMM adalah kerangka untuk mengembangkan proses, seperti proses teknis baik informal maupun formal. Pembobotan yang digunakan mengadopsi dari penilaian resiko.Menurut Sarno dan Iffano (2009: 89) dalam hubungannya dengan SMKI, resiko adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi di organisasi, yang dimaksud adalah ancaman terhadap aspek keamanan informasi yaitu CIA (Confidentiality, Integrity, Availability). Sehingga setiap pernyataan akan diberikan bobot sesuai dengan nilai resiko yang akan terjadi apabila tidak diterapkan.

METODOLOGI PENELITIAN

Langkah-langkah pelaksanaan audit keamanan sistem informasi mencangkup:

1. Penentuan ruang lingkup
2. Pengumpulan data.
3. Pelaksanaan audit kepatutan.
4. Penentuan *maturity level*.
5. Penentuan hasil audit keamanan sistem informasi.
6. Penyusunan laporan hasil audit keamanan sistem informasi.

IMPLEMENTASI DAN HASIL

Penentuan Ruang Lingkup Audit Keamanan Sistem Informasi

Ruang lingkup audit keamanan sistem informasi berdasarkan peraturan Bank Indonesia (BI) dalam pedoman untuk menerapkan manajemen resiko dalam penggunaan TI dan disesuaikan dengan kriteria audit yang menggunakan standar ISO 27001. Tabel 1 merupakan pemetaan dari pedoman yang digunakan terhadap klausul-klausul ISO 27001.

Tabel 1 Pemetaan Klausul ISO27001

Pedoman BI	Klausul
Prosedur Pengelolaan Aset	7
Prosedur Pengelolaan SDM	8
Prosedur Pengamanan Fisik dan Lingkungan	9
Prosedur Pengamanan *Logical Security*	10
Prosedur Pengamanan Operasional Teknologi Informasi	11,12
Prosedur Penanganan Insiden dalam Pengamanan Informasi	13

Pelaksanaan Audit Kepatutan dan Penentuan Maturity Level

Pelaksanaan audit kepatutan menghasilkan dokumen wawancara, bukti-bukti audit, temuan audit dan nilai tingkat kematangan tiap kontrol keamanan. Dokumen wawancara diperoleh saat prosedur pembuatan pertanyaan dari pernyataan yang sebelumnya dibuat. Bukti-bukti dan temuan audit diperoleh saat dilakukan wawancara kepada perusahaan. Setelah didapatkan bukti-bukti dan temuan audit tersebut kemudian dievaluasi dan dianalisa lalu menentukan nilai tingkat kemampuan tiap-tiap kontrol keamanan.

Contoh kerangka kerja perhitungan nilai *maturity level* dapat dilihat pada Tabel 2, untuk contoh hasil perhitungan tingkat kemampuan dapat dilihat pada Tabel 3 dan contoh representasi hasilnya ke dalam digram radar dapat dilihat pada Gambar 1.

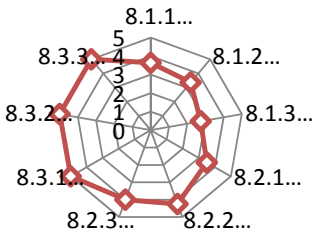
Tabel 2 Contoh Kerangka Kerja Perhitungan *Maturity Level*

8.3.2	Pengembalian Aset								
No	Pernyataan	Bobot	0	1	2	3	4	5	Nilai
1	Pengembalian aset pegawai telah dilakukan sesuai kontrak pada saat berhenti kerja.	1						√	5
2	Pengembalian aset pegawai telah dilakukan sesuai kontrak pada saat dipindahkan.	1						√	5
Total Bobot		2	Tingkat Kemampuan						5

Tabel 3 Contoh Hasil *Maturity Level Klausul* 8 Manajemen SDM

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata/Objektif Kontrol
8 Manajemen Sumber Daya Manusia	8.1 Keamanan SDM Sebelum Menjadi Pegawai	8.1.1 Aturan dan Tanggung Jawab	3,64	3,25
		8.1.2 Seleksi	3,36	
		8.1.3 Persyaratan dan Kondisi Yang Harus Dipenuhi Oleh Pegawai	2,75	
	8.2 Selama Menjadi Pegawai	8.2.1 Tanggung Jawab Manajemen	3,50	3,92
		8.2.2 Pendidikan	4,25	

		dan Pelatihan Keamanan Informasi		
Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata/Objektif Kontrol
		8.2.3 Proses Kedisiplinan	4,00	
	8.3 Pemberhentian atau Pemindahan Pegawai	8.3.1 Tanggung Jawab Pemberhentian	5,00	5,00
		8.3.2 Pengembalian Aset	5,00	
		8.3.3 Penghapusan Hak Akses	5,00	
	Maturity Level Klausul 8			4,06



Gambar 1 Contoh Representasi Nilai *Maturity Level* Klausul 8 Manajemen SDM

Penentuan dan Penyusunan Hasil Audit Sistem Informasi

Hasil audit keamanan sistem informasi berupa temuan dan rekomendasi untuk perusahaan. Temuan dan rekomendasi tersebut berasal dari hasil wawancara yang dilakukan, yang sebelumnya dievaluasi dan dianalisa.Laporan hasil audit yang berupa temuan-temuan dan rekomendasi tersebut digunakan sebagai saran untuk perbaikan kontrol keamanan.

Setelah seluruh perhitungan selesai didapatkan nilai maturity level dari rata-rata keseluruhan nilai klasul yang dapat dilihat pada Tabel 4.

Tabel 4 Hasil *Maturity Level* Seluruh Klausul

Klausul	*Maturity Level*
7	1.91
8	4.06
9	2.96
10	3.54
11	2.93
12	2.94
13	1.96
Nilai *Maturity Level*	2.90

Didapat representasi hasil *maturity level* seluruh klausul pada Gambar 2 dan terlihat bahwa Manajemen Aset dan Kejadian Keamanan Informasi memiliki nilai yang belum baik, sehingga harus dimanajemen ulang pada prosedur untuk mengelola kontrol keamanannya.

Gambar 2 Representasi Hasil *Maturity Level* Seluruh Klausul

Penyusunan Temuan

Setelah dilakukan analaisa dan evaluasi dari audit keamanan sistem informasi pada PT. BPR JATIM didapatkan beberapa kondisi yang telah sesuai dengan kontrol keamananan pada ISO 27001 yang telah ditetapkan. Beberapa kondisi tersebut yaitu:

1. Terdapat aturan mengenai tanggung jawab keamanan informasi pada kontrak kerja pegawai.
2. Terdapat perimeter keamanan untuk melindungi ruang yang berisikan fasilitas pemrosesan informasi.
3. Terdapat dokumentasi terhadap prosedur operasi.
4. Terdapat dokumentasi penetapan persyaratan bisnis untuk kontrol akses.
5. Terdapat persyaratan kebutuhan keamanan sistem informasi pada sistem baru.

Sedangkan kondisi yang masih perlu perbaikan yaitu:

1. Penjadwalan pengontrolan aset belum dilakukan secara berkala dan belum ada bagian atau individu tertentu yang bertugas mengontrol aset.
2. Belum ada peran penanggung jawab khusus untuk perlindungan aset tertentu.
3. Belum ada panduan mekanisme kontrol untuk perlindungan pada keamanan fisik.
4. Belum dilakukan pengontrolan dan pencatatan terhadap perubahan fasilitas pemrosesan informasi.
5. Kaji ulang hak akses, otorisasi hak khusus dan alokasinya belum dilakukan secara berkala.

Penyusunan Rekomendasi

Berdasarkan dari temuan yang didapat dari audit keamanan sistem informasi maka disusun rekomendasi guna perbaikan untuk kondisi-kondisi pada perusahaan yang belum sesuai dengan prosedur. Beberapa rekomendasi tersebut yaitu:

1. Mengiidentifikasi dengan jelas dan menginventarisasi seluruh aset yang dimiliki oleh organisasi.
2. Mengklarifikasikan dan membuat panduan klasifikasi Informasi agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.
3. Membuat prosedur penandaan klasifikasi misalnya informasi ”rahasia” (misalnya data simpanan nasabah, data pribadi nasabah), ”internal” (misalnya peraturan tentang gaji pegawai Bank) dan ”biasa” (misalnya informasi

tentang produk perbankan yang ditawarkan ke masyarakat).

Kesimpulan

Berdasarkan hasil audit keamanan sistem informasi, maka didapat kesimpulan:

1. Perencanaan audit keamanan sistem informasi pada PT. BPR JATIM menghasilkan identifikasi ruang lingkup pada pedoman Bank Indonesia dalam menerapkan manajemen resiko pada TI. Pengumpulan data dilakukan dengan wawancara untuk menentukan dokumen-dokumen yang diperlukan. Langkah pelaksanaan audit keamanan sistem informasi dilakukan dengan pembuatan pernyataan, penentuan nilai bobot, pembuatan pertanyaan dan penentuan nilai kematangan.
2. Pelaksanaan audit keamanan sistem informasi dengan pengumpulan data memperoleh dokumen hasil wawancara.
3. Hasil maturity level didapat dari seluruh kontrol keamanan mendapatkan nilai sebesar 2,90 yang berarti bahwa kontrol keamanan masih berada pada level 2 *planned and tracked* (direncanakan dan dilacak) namun telah mendekati level 3 *well defined* (didefinisikan dengan baik) yang merupakan level yang diharapkan oleh perusahaan, sehingga diperlukan peningkatan kontrol keamanan yang telah direkomendasikan.

Saran

Beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut yaitu:

1. Audit keamanan sistem informasi belum menerapkan seluruh kontrol keamanan yang sesuai dengan pedoman BI, karena perusahaan baru saja mengalami perubahan sistem sehingga masih dalam tahap pengembangan. Untuk itu diharapkan setelah seluruh sistem perusahaan telah berjalan sesuai dengan proses bisnis yang ada atau bahkan telah membuat prosedur sistem manajemen keamanan informasi maka perlu dilakukan audit keamanan sistem informasi kembali.
2. Audit keamanan sistem informasi ini menggunakan standar ISO 27001 dan penilaian maturity level menggunakan SSE-CMM, dikarenakan ISO memang belum memiliki metode penilaian maka dari itu untuk pengembangan penelitian selanjutnya dapat menggunakan *maturity model* lain untuk bahan perbandingan.

Daftar Pustaka

Direktorat Penelitian dan Pengaturan Perbankan.2007. Pedoman Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Jakarta. Bank Indonesia.

Gondodiyoto, S. 2007. Audit Sistem Informasi Pendekatan COBIT. Jakarta: Mitra Wacana Media.

Gunawan, H dan Suhono, R D. 2006. *Studi ISO 17799:2005 Dan Systems Security Engineering Capability Maturity Model (SSE-CMM) Untuk Keamanan Aplikasi Web.* Bandung: Institut Teknologi Bandung.

Jogianto, H,M. 2005. Analisa dan Desain. Yogyakarta: Andi

Sarno, Riyanarto. 2009. Audit Sistem & Teknologi Informasi. Surabaya: ITS Press.

Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.